REMARKS

Upon entry of the foregoing amendment, Claims 1-12 are pending in the application, with Claims 1 and 7 being the independent claims.

Claims 1, 2, 4, 6, 7, 8, 10 and 12 have been amended in order to more particularly point out and distinctly claim the subject matter the Applicants regard as their invention. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Claims 13-41 have been canceled without prejudice to, or disclaimer of, the subject matter therein. More specifically, these claims have now been formally canceled in accordance with the Examiner's Restriction requirement under 35 U.S.C. § 121 and Applicants' January 24-25, 2001, oral election of the Group I claims (*i.e.,* Claims 1-12). *See* Office Action at paragraphs 2.1 and 2.3.

The Applicants wish to thank the Examiner for an informative Interview held on May 22, 2001.

Based on the above Amendment and the following Remarks, Applicants respectfully request that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Request for Information under 37 C.F.R. § 1.105

Along with the Office Action, the Examiner issued a Request for Information under 37 C.F.R. § 1.105 (hereinafter "Request"). Applicants now respond to the Request.

First, the Examiner has requested "the names of any products or services that have incorporated the claimed subject matter." Request at paragraph 4. In response, Applicants hereby represent that no products or services, other than that discussed in the May 22, 2001, Interview, have incorporated the claimed subject matter.

Second, the Examiner has requested "the citation and a copy of each publication that any

of the applicants relied upon to develop the disclosed subject matter . . . particularly as to developing the calculation of a risk or a relative risk of a terrorist attack based on a site accessability and probability." Request at paragraph 5. In response, Applicants hereby identify the following documents:

(1)   Department of Defense, DoD Instruction 2000.16, *DoD Combating Terrorism Program Standards*, July 21, 1997.

(2)   Department of Defense, DoD 0-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*, February 1993, Chapters 5-14, 16, and 22.

(3)   Chairman of the Joint Chiefs of Staff, Joint Chiefs of Staff Handbook 5260, *Commander's Handbook for Antiterrorism Readiness*, January 1, 1997, Chapters 3-5.

(4)   Joint Chiefs of Staff, Joint Publication No. 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, Mar. 17, 1998, pages II-1 - II-12, IV-1 - V-10, and VII-1 - VII-10.

An Information Disclosure Statement (IDS) and Form PTO-1449 listing document (4) is submitted concurrently herewith.[1] The relevancy of these four documents, as suggested in the specification (*see, e.g.,* page 4), is that they contain background on the general methodologies and specific risk concepts involved in the antiterrorism arts. *See* 37 C.F.R. § 1.105(a)(1)(v).

Rejections Based on 35 U.S.C. § 112, Paragraph 2

The Examiner rejected pending Claims 1-12 under 35 U.S.C. § 112, paragraph 2, as being indefinite for containing the term "relative risk." Office Action at paragraph 6.1. Thus, Claims 1, 2, 4, 6, 7, 8, 10 and 12 have been amended in accordance with the Examiner's suggestions to more particularly point out and distinctly claim the subject matter the Applicants regard as their invention.

---

[1]   Documents (1)-(3) are marked "FOR-OFFICIAL-USE-ONLY" by the Department of Defense and thus not attached to the IDS. The Examiner, as a federal employee, is invited to make arrangements to obtain these documents.

Rejections Based on 35 U.S.C. § 112, Paragraph 1

The Examiner also rejected pending Claims 1-12 under 35 U.S.C. § 112, paragraph 1, as "containing subject matter which was not described in the specification in such a way as to enable one skilled in the [art] to which it pertains, or with which it is most nearly connected, to make and/or use the invention." Office Action at paragraph 5.1. Applicants respectfully traverse these rejections below.

Background

First, in preferred embodiments, the present invention takes the form of a software program that may be run on a personal computer or workstation that allows users to evaluate the risk of a terrorist attack at their site, determine their vulnerability to a terrorist attack, assess the damage caused by a successful terrorist attack, and select countermeasures to prevent terrorist attacks.

Second, given the above, the Examiner is reminded that the specification must enable one skilled in the technology that is relevant to the invention so that it may be practiced. *See In re Naquin*, 158 U.S.P.Q. 317 (C.C.P.A. 1968). Consequently, if an invention involves aspects relating to several different arts, then the specification should enable persons skilled in each art to carry out their respective aspect of the invention. *Id.* at 319. The MPEP reflects this state of the law by reminding us that:

> In computer applications, it is not unusual for the claimed invention to involve two areas of prior art or more than one technology, e.g., an appropriately programmed computer and an area of application of said computer. In regard to the "skilled in the art" standard in cases involving both the art of computer programming, and another technology, the examiner must recognize that knowledge of persons skilled in both technologies is the appropriate criteria for determining sufficiency.

MPEP § 2106.02 (citations omitted). Therefore, given the present invention, the "one skilled in the art" is actually two persons--one skilled in artificial intelligence computer programming and

one skilled in the area of antiterrorism.

Third, the ultimate question under 35 U.S.C. § 112, first paragraph is whether the specification contains sufficient information to enable one skilled in the art to practice the invention without undue experimentation. *PPG Indus. v. Guardian Indus. Corp.*, 37 U.S.P.Q.2d 1618, 1623 (Fed. Cir. 1996). However, it is important to note: "That some experimentation is necessary does not constitute a lack of enablement; the amount of experimentation, however, must not be *unduly extensive*." *Amgen, Inc. v. Chugai Pharm. Co., Ltd.*, 18 U.S.P.Q.2d 1016, 1026 (Fed. Cir. 1991) (emphasis added). The Federal Circuit has explained that:

> Enablement is not precluded by the necessity for some experimentation such as routine screening. However, experimentation needed to practice the invention *must not be undue experimentation*. The key word is "undue," not experimentation. . . . Whether undue experimentation is needed is not a single, simple factual determination, but rather is a *conclusion reached by weighing many factual considerations*.

In re Wands, 8 U.S.P.Q.2d 1400, 1404 (Fed. Cir. 1988) (emphasis added).[2]

Given the above, the Examiner is reminded that in the field of artificial intelligence, some experimentation is always present. *See, e.g.,* Kathryn B. Laskey and Suzanne M. Mahoney, "Network Engineering for Agile Belief Network Models," *Proceedings of the Twelfth Conference on Uncertainty in Artificial Intelligence*, Portland, OR, Morgan Kaufman pubs. (July 31-Aug. 3, 1996) (hereinafter Laskey), which is attached hereto as Exhibit A. That is, it is admitted that the application of the present invention, like all artificial intelligence applications, is dependent on expert knowledge and/or historical data pertaining to the subject matter at hand.

---

[2] The court went on to state factors that may be employed determining whether a disclosure requires undue experimentation. These factors "include (1) the quantity of experimentation necessary, (2) the amount of direction or guidance presented, (3) the presence or absence of working examples, (4) the nature of the invention, (5) the state of the prior art, (6) the relative skill of those in the art, (7) the predictability or unpredictability of the art, and (8) the breadth of the claims." *Id.* at 1404.

The Examiner's Rejections

The Examiner contends that: "The disclosure describes a method and system used to determine a risk based on a determination of an accessibility of a site and a probability that a terrorist attack will occur. However, the disclosure fails to provide guidance regarding the calculations of accessibility and probability to permit one skilled in the art to make and/or use invention, without undue experimentation." Office Action at paragraph 5.2. Applicants respectfully disagree.

First, a preferred embodiment of the Influence Network is presented in Figure 5. That figure shows the major components that influence risk, but the exact configuration of the network is no more or less relevant to the design of the apparatus as are specific data to drive the simulations such as weights and maximum speeds of vehicles. One skilled in the relevant art(s) would use the Specification to build the apparatus to assess risk to terrorist attack based on the high-level nodes presented in Figure 5 (510 and 510a). Details of the parents of those nodes are a matter of detailed implementation by subject matter experts, a practice that is well understood in the artificial intelligence community.

Second, Figure 5 of the Specification illustrates the major nodes that are used as part of the method for risk analysis being claimed. The specific complexity of the resulting network is dependent on the specific embodiment of the apparatus and method as determined by the end user. The apparatus and method being claimed facilitate the population of the Influence Network through the architecture presented in the Specification.

Third, it is common practice to engineer the knowledge inherent in a Bayesian Influence Network. *See* Laskey at pages 8-11. Thus, as will be appreciated by one skilled in the relevant art(s) it would be inappropriate to attempt to define the probability and statistics equations, nodes states, and conditional probabilities in the Specification because they are subject to constant

-8-

change and update by the user and will be different from user to user, while staying within the same overarching method.

Fourth, it is admitted that the network requires experts in the field of antiterrorism to engineer the network. This is common practice, however, in all fields of artificial intelligence--not just Bayesian networks. There are well-known and well-published methods for knowledge engineering to complete the specifics of an artificial intelligence application. *See* Laskey at pages 9-10.

The Examiner also contends that: "A review of the Specification indicates that probability and risk calculation are made using a Bayesian network in conjunction with a set of probability and statistics equations. Although the Specification provides some guidance regarding the structure of the network used, the Specification fails to provide information necessary to construct a Bayesian network that produces accurate results." Office Action at paragraph 5.3. Given the traversal of the Examiner's contentions in paragraph 5.2 of the Office Action above, the Applicant's respectfully disagree. That is, the exact construction of any given instance of the Bayesian network is not relevant to the method and apparatus being claimed. *See* Laskey at pages 12-15.

Apparatus Claims 1-6

With respect to Claims 1-6, the claimed apparatus for assessing risk of a terrorist attack claimed is represented clearly in several figures in the Specification and their accompanying text. That is, Figure 2 shows the architecture of the Apparatus being claimed. As shown in this figure, the architecture integrates nine (9) key components to determine risk. Of these components, the Computational Engine 230 handles the calculations of risk, as indicated on pages 22-24 and 53-55 of the Specification. As the Specification indicates, the computational engine facilitates the process of "informing" the Bayesian network by coordinating inputs from the GUI 202, the

Plug-in Interface 250, the Dynamics Module 240, and the Database 220.

Additionally, the Specification and Figures teach the following:

· Figure 21 shows how the Computational Engine and Dynamics modules calculate accessibility to inform the Bayesian Influence Network.
· Figures 37-38 further define how the Dynamics Module calculates accessibility. Values of accessibility can also be entered by directly by the user as indicated in Figure 36.
· Figure 35 shows how the Computational Engine determines Susceptibility and determines the effect of Countermeasures on risk to inform the Bayesian Influence Network
· Figure 36 shows how the Computational Engine informs the Bayesian influence network with judgements entered by the user as well as calculations made within the apparatus
· Figure 9 shows how external analytic models connect to the apparatus allowing calculations of consequences and other Bayesian Network Nodes to be populated.
· Figure 46 shows details of how external analytic models interact with the apparatus through the Plug-In Interface.

Method Claims 7-12

As to Claims 7-12, the method for assessing risk of a terrorist attack claimed is

represented clearly in several figures in the Specification and their accompanying text. For

example:

· Figure 22 shows the process by which the apparatus allows risk management
· Figure 28 shows how the Influence Network can be populated
· Figure 33 shows how the process of risk analysis and management leads to a plan
· Figure 34 shows how the process of risk analysis in Figure 33 is facilitated by the influence network.

Given the foregoing, Applicants assert that the Specification and accompanying Figures

enable those skilled in the relevant art(s) to make and/or use the present invention as claimed in

Claims 1-12.

CONCLUSION

The Examiner has indicated that Claims 1-12 are allowable subject matter contingent upon the above-traversed rejections. *See* Office Action at paragraph 7. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. The Examiner is invited to contact the undersigned by telephone should the Examiner believe that personal communication will expedite prosecution of this application.

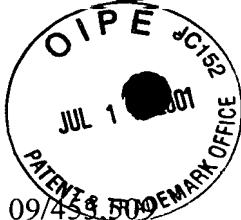Respectfully submitted,

PIPER MARBURY RUDNICK & WOLFE LLP

Steven B. Kelber
Registration No. 30,073
Attorney of Record

Raymond Millien
Registration No. 43,806

1200 Nineteenth Street, N.W.
Washington, D.C. 20036-2412
Telephone No. (202) 861-3900
Facsimile No. (202) 223-2085

-11-

MARKED-UP COPY OF AMENDED CLAIMS

1. (Amended) An apparatus for assessing a risk of a terrorist attack comprising:

a memory;

an input device;

a display device; and

a processor connected to the memory, the input device and the display device, the processor being configured to perform the steps of:

inputting information about a site of potential terrorist attack from a user;

constructing a model of the site based on the information input from the user;

accepting a designation from the user of a weapon and delivery point at the site;

determining an accessability of the site to the weapon/delivery point by determining a threat vector which is mostly likely the threat vector by which the weapon will be delivered and the likelihood of a successful delivery based on the model;

determining a probability that a terrorist attack will occur; and

calculating a [relative] risk based at least partially on the accessibility and probability.

2. (Amended) The apparatus of Claim 1, wherein the [relative] risk is further based on a consequence calculation.

4. (Amended) The apparatus of Claim 1, wherein the processor is further configured to perform the step of preparing a report including the probability, accessability and [relative] risk.

6. (Amended) The apparatus of Claim 1, wherein the [relative] risk is calculated using a Bayesian network.

7. (Amended) A method for assessing a risk of a terrorist attack comprising the steps of:

inputting information about a site of a potential terrorist attack from a user;

constructing a model of the site based on the input from the user;

accepting a designation from the user of a weapon and delivery point at the site;

determining an accessability of the site to the weapon/delivery point by determining a threat vector which is mostly likely the threat vector by which the weapon will be delivered and the likelihood of a successful delivery based on the model;

determining a probability that a terrorist attack will occur; and

calculating a [relative] risk based at least partially on the accessibility and probability.

8. (Amended) The method of Claim 7, wherein the [relative] risk is further based on a consequence calculation.

10. (Amended) The method of Claim 7, wherein the processor is further configured to perform the step of preparing a report including the probability, accessability and [relative] risk.

12. (Amended) The method of Claim 7, wherein the [relative] risk is calculated using a Bayesian network.